



**Queensland University of Technology**  
Brisbane Australia

This is the author's version of a work that was submitted/accepted for publication in the following source:

Boyen, Xavier (2003) Multipurpose identity-based signcryption : a Swiss army knife for identity-based cryptography. In *Advances in Cryptology - CRYPTO 2003 : Proceedings of the 23rd Annual International Cryptology Conference*, Springer Verlag, Santa Barbara, California, USA, pp. 383-399.

This file was downloaded from: <http://eprints.qut.edu.au/58800/>

**© Copyright 2003 International Association for Cryptologic Research**

The original publication is available at [www.springerlink.com](http://www.springerlink.com)

**Notice:** *Changes introduced as a result of publishing processes such as copy-editing and formatting may not be reflected in this document. For a definitive version of this work, please refer to the published source:*

# Efficient and Secure Identity-Based Signatures and Signcryption from Bilinear Maps

Paulo S. L. M. Barreto<sup>2</sup>, Benoît Libert<sup>3</sup>,  
Noel McCullagh<sup>1</sup>, and Jean-Jacques Quisquater<sup>3</sup>

<sup>1</sup> School of Computer Applications  
Dublin City University  
Ballymun, Dublin 9, Ireland.  
`noel.mccullagh@computing.dcu.ie`

<sup>2</sup> PCS, Escola Politécnica, Universidade de São Paulo  
Av. Prof. Luciano Gualberto, tr. 3, n. 158, s. C1-46  
BR 05508-900, São Paulo(SP), Brazil.  
`pbarreto@larc.usp.br`

<sup>3</sup> UCL, Microelectronics Laboratory, Crypto Group  
Place du Levant, 3, B-1348, Louvain-La-Neuve, Belgium.  
Telephone : +32(0)10 47.80.62, Fax : +32(0)10 47.25.98  
`benoit.libert, jean-jacques.quisquater@uclouvain.be`

**Abstract.** In this work we describe new identity-based signature and combined signature/encryption (signcryption) schemes built upon bilinear maps. These schemes turn out to be more efficient than all others proposed so far. We prove their security in a proper security model under recently studied computational assumptions and in the random oracle model. We then give implementation results to illustrate the significance of our improvements w.r.t. previous proposals.

## 1 Introduction

Identity based cryptography has become a very fashionable area of research for the last couple of years. The concept was originally introduced in 1984 by Shamir [41] whose idea was that users within a system could use their online identifiers (combined with certain system-wide information) as their public keys. This greatly reduces the problems with key management that have hampered the mass uptake of public key cryptography on a per individual basis. While identity-based signature schemes (IBS) rapidly emerged [25, 29] after 1984 (see [6] for a thorough study of them), and despite another bandwidth-consuming proposal [22], it is only in 2001 that bilinear mappings over elliptic curve were found to yield the first fully practical identity-based encryption (IBE) solution [12]. Those bilinear maps, or pairings, subsequently turned out to yield a plenty of cryptographic applications [2] among which several recent outstanding results on identity-based encryption [8, 9, 26, 43, 11, 27, 14].

This work proposes a new very efficient method, often referred to as 'signcryption' in the literature [46, 1], to jointly achieve signature and encryption

with identifier-based public keys. Several identity-based signcryption (IBSC) algorithms have been proposed so far, e.g. [13, 17, 20, 21, 32, 33, 36, 40, 44]. Within this handful of results, only [13, 17, 20, 21, 32, 44] considered schemes supported by formal models and security proofs in the random oracle model [7]. Among them, Chen and Malone-Lee’s proposal [17] was the most efficient construction.

Our main achievement is to propose a new identity-based signcryption scheme that even supersedes [17] from an efficiency point of view at the expense of a security resting on stronger assumptions. The new construction can benefit from the most efficient pairing calculation techniques for a larger variety of elliptic curves than previous schemes. Indeed, recent observations [42] pinpointed problems arising when many provably secure pairing-based protocols are implemented using asymmetric pairings and ordinary curves. Our proposal avoids those problems thanks to the fact that it does not require to hash onto an elliptic curve cyclic subgroup. As a result of independent interest, we discovered a new identity-based signature that happens to be faster at verification than previously known IBS schemes.

This document is organized as follows. Section 2 presents the basic security theoretic concepts of bilinear map groups and the hard problems underlying our proposed algorithms. We describe our identity-based signature scheme and prove its security in section 3. We propose our new identity-based signcryption scheme in section 4. Its known disadvantages are discussed in section 5 and we compare its efficiency to various schemes in section 6. We address intellectual property issues in section 7 and draw our conclusions in section 8.

## 2 Preliminaries

### 2.1 Bilinear map groups and related computational problems

Let  $k$  be a security parameter and  $p$  be a  $k$ -bit prime number. Let us consider groups  $\mathbb{G}_1$ ,  $\mathbb{G}_2$  and  $\mathbb{G}_T$  of the same prime order  $p$  and let  $P, Q$  be generators of respectively  $\mathbb{G}_1$  and  $\mathbb{G}_2$ . We say that  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  are *bilinear map groups* if there exists a bilinear map  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  satisfying the following properties:

1. Bilinearity:  $\forall (S, T) \in \mathbb{G}_1 \times \mathbb{G}_2, \forall a, b \in \mathbb{Z}, e(aS, bT) = e(S, T)^{ab}$ .
2. Non-degeneracy:  $\forall S \in \mathbb{G}_1, e(S, T) = 1$  for all  $T \in \mathbb{G}_2$  iff  $S = \mathcal{O}$ .
3. Computability:  $\forall (S, T) \in \mathbb{G}_1 \times \mathbb{G}_2, e(S, T)$  is efficiently computable.
4. There exists an efficient, publicly computable (but not necessarily invertible) isomorphism  $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$  such that  $\psi(Q) = P$ .

Such bilinear map groups are known to be instantiable with ordinary elliptic curves such as those suggested in [35] or [5]. In this case, the trace map can be used as an efficient isomorphism  $\psi$  as long as  $\mathbb{G}_2$  is properly chosen [42]. With supersingular curves, symmetric pairings (i.e.  $\mathbb{G}_1 = \mathbb{G}_2$ ) can be obtained and  $\psi$  is the identity.

The computational assumptions for the security of our schemes were previously formalized by Boneh and Boyen [8] and are recalled in the following definition.

**Definition 1** ([8]). Let us consider bilinear map groups  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  and generators  $P \in \mathbb{G}_1$  and  $Q \in \mathbb{G}_2$ .

The **q-Diffie-Hellman Inversion** problem (*q-DHIP*) in  $(\mathbb{G}_1, \mathbb{G}_2)$  consists in, given a  $(q+2)$ -tuple  $(P, Q, \alpha Q, \alpha^2 Q, \dots, \alpha^q Q)$ , finding  $\frac{1}{\alpha}P$ .

The **q-Bilinear Diffie-Hellman Inversion** problem (*q-BDHIP*) in the groups  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  consists in, given  $(P, Q, \alpha Q, \alpha^2 Q, \dots, \alpha^q Q)$ , computing  $e(P, Q)^{1/\alpha} \in \mathbb{G}_T$ .

Although these problems may be easier than originally expected in some cases [18], they are still assumed to be hard in practice and lower bounds for their complexity in generic groups were given in [10, 24].

### 3 A new identity-based signature

We here present a new identity-based signature that is significantly more efficient all known pairing based IBS schemes as its verification algorithm requires a single pairing calculation. This efficiency gain is obtained at the expense of letting the security rely on a stronger assumption than other provably secure pairing based IBS [15, 19, 30].

**Setup:** given a security parameter  $k$ , the PKG chooses bilinear map groups  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  of prime order  $p > 2^k$  and generators  $Q \in \mathbb{G}_2$ ,  $P = \psi(Q) \in \mathbb{G}_1$ ,  $g = e(P, Q)$ . It then selects a master key  $s \xleftarrow{R} \mathbb{Z}_p^*$ , a system-wide public key  $Q_{pub} = sQ \in \mathbb{G}_2$  and hash functions  $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ ,  $H_2 : \{0, 1\}^* \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$ . The public parameters are

$$\text{params} := \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, Q, g, Q_{pub}, e, \psi, H_1, H_2\}$$

**Keygen:** for an identity  $ID$ , the private key is  $S_{ID} = \frac{1}{H_1(ID)+s}P$ .

**Sign:** in order to sign a message  $M \in \{0, 1\}^*$ , the signer

1. picks a random  $x \xleftarrow{R} \mathbb{Z}_p^*$  and computes  $r = g^x$ ,
2. sets  $h = H_2(M, r) \in \mathbb{Z}_p^*$ ,
3. computes  $S = (x + h)S_{ID}$ .

The signature on  $M$  is  $\sigma = (h, S) \in \mathbb{Z}_p^* \times \mathbb{G}_1$ .

**Verify:** a signature  $\sigma = (h, S)$  on a message  $M$  is accepted iff

$$h = H_2(M, e(S, H_1(ID)Q + Q_{pub})g^{-h}).$$

The scheme can be thought of as an identity-based extension of a digital signature discussed in two independent papers [10, 45]. More precisely, the method for obtaining private keys from identities is a simplification of a method suggested by Sakai and Kasahara [40].

In [31], Kurosawa and Heng described an identity-based identification (IBI) protocol that implicitly suggests an IBS described in appendix E and which can be proven secure under the same assumption as our proposal. It turns out that

ours is slightly faster than the Kurosawa-Heng IBS in the signature generation.

At Eurocrypt'04, Bellare, Namprempe and Neven established a framework [6] for proving the security of a large family of identity-based signatures and they only found two schemes to which their framework does not apply. The present one does not either fall into the category of schemes to which it applies. Indeed, it can be showed that our IBS does not result from the transformation of any convertible standard identification or signature scheme (in the sense of [6]) unless the  $q$ -Strong Diffie-Hellman problem [10] is easy<sup>1</sup>. A direct security proof is thus needed.

### 3.1 Security results

We recall here the usual model [6, 15, 19, 23, 30] of security for identity-based signatures which is an extension of the usual notion of existential unforgeability under chosen-message attacks [28].

**Definition 2 ([15]).** *An IBS scheme is **existentially unforgeable** under adaptive chosen message and identity attacks if no probabilistic polynomial time (PPT) adversary has a non-negligible advantage in this game:*

1. *The challenger runs the setup algorithm to generate the system's parameters and sends them to the adversary.*
2. *The adversary  $\mathcal{F}$  performs a series of queries to the following oracles:*
  - *Key extraction oracle: returns private keys for arbitrary identities.*
  - *Signature oracle: produces signatures on arbitrary messages using the private key corresponding to arbitrary identities.*
3.  *$\mathcal{F}$  produces a triple  $(ID^*, M^*, \sigma^*)$  made of an identity  $ID^*$ , whose private key was never extracted, and a message-signature pair  $(M^*, \sigma^*)$  such that  $(M^*, ID^*)$  was not submitted to the signature oracle. She wins if the verification algorithm accepts the triple  $(ID^*, M^*, \sigma^*)$ .*

The next lemmas establish the security of the scheme under the  $q$ -DHI assumption. Lemma 1 [15] allows to only consider a weaker attack where a forger is challenged on a given identity chosen by the challenger. The proof of lemma 2 relies on the forking lemma [38, 39].

In our original paper [3], we gave a security proof under the  $q$ -Strong Diffie-Hellman assumption. Here, we provide a new proof under the weaker  $q$ -DHI assumption.

**Lemma 1 ([15]).** *If there is a forger  $\mathcal{F}_0$  for an adaptively chosen message and identity attack having advantage  $\epsilon_0$  against our scheme when running in a time  $t_0$  and making  $q_{h_1}$  queries to random oracle  $h_1$ , then there exists an algorithm  $\mathcal{F}_1$  for an adaptively chosen message and given identity attack which has advantage  $\epsilon_1 \leq \epsilon_0(1 - \frac{1}{2^k})/q_{h_1}$  within a running time  $t_1 \leq t_0$ . Moreover,  $\mathcal{F}_1$  asks the same number key extraction queries, signature queries and  $H_2$ -queries as  $\mathcal{F}_0$  does.*

<sup>1</sup> This problem is to find a pair  $(c, \frac{1}{c+\alpha}P) \in \mathbb{Z}_p^* \times \mathbb{G}_1$  given  $(P, Q, \alpha Q, \alpha^2 Q, \dots, \alpha^q Q)$ . It is obviously not harder than the  $q$ -DHI problem where  $c$  is set to 0 and may not be freely chosen.

**Lemma 2.** *Let us assume that there is an adaptively chosen message and given identity attacker  $\mathcal{F}$  that makes  $q_{h_i}$  queries to random oracles  $H_i$  ( $i = 1, 2$ ) and  $q_s$  queries to the signing oracle. Assume that, within a time  $t$ ,  $\mathcal{F}$  produces a forgery with probability  $\epsilon \geq 10(q_s + 1)(q_s + q_{h_2})/2^k$ . Then, there exists an algorithm  $\mathcal{B}$  that is able to solve the  $q$ -DHIP for  $q = q_{h_1}$  in an expected time*

$$t' \leq 120686q_{h_2}(t + O(q_s\tau_p))/(\epsilon(1 - q/2^k)) + O(q^2\tau_{\text{mult}})$$

where  $\tau_{\text{mult}}$  denotes the cost of a scalar multiplication in  $\mathbb{G}_2$  and  $\tau_p$  is the cost of a pairing evaluation.

*Proof.* See appendix A. □

The combination of the above lemmas yields the following theorem.

**Theorem 1.** *Let us assume that there exists an adaptively chosen message and identity attacker  $\mathcal{F}$  making  $q_{h_i}$  queries to random oracles  $H_i$  ( $i = 1, 2$ ) and  $q_s$  queries to the signing oracle. Assume that, within a time  $t$ ,  $\mathcal{F}$  produces a forgery with probability  $\epsilon \geq 10(q_s + 1)(q_s + q_{h_2})/2^k$ . Then, there exists an algorithm  $\mathcal{B}$  that is able to solve the  $q$ -DHIP for  $q = q_{h_1}$  in an expected time*

$$t' \leq 120686q_{h_1}q_{h_2}(t + O(q_s\tau_p))/(\epsilon(1 - q/2^k)) + O(q^2\tau_{\text{mult}})$$

where  $\tau_{\text{mult}}$  and  $\tau_p$  respectively denote the cost of a scalar multiplication in  $\mathbb{G}_2$  and the required time for a pairing evaluation.

In the proof, the reduction is unfortunately far from being tight. However, security reductions for identity-based signatures in the random oracle model generally tend to be loose (mainly because of the use of the forking lemma [38, 39]). Besides, the practical relevance of a tight reduction in the random oracle model is unclear. Moreover, the only known secure IBS scheme [37] in the standard model (i.e. without random oracles) does not have tight reductions either.

## 4 Fast identity-based signcryption

Before describing our new scheme, we first give functional definitions and properly model security notions for identity-based signcryption schemes.

### 4.1 Formal model of identity-based signcryption

The formal structure that we shall use for IBSC schemes is the following.

**Setup:** is a probabilistic algorithm run by a private key generator (PKG) that takes as input a security parameter to output public parameters **params** and a master key **mk** that is kept secret.

**Keygen:** is a key generation algorithm run by the PKG on input of **params** and the master key **mk** to return the private key  $S_{\text{ID}}$  for the identity **ID**.

**Sign/Encrypt:** is a probabilistic algorithm that takes as input public parameters  $\text{params}$ , a plaintext message  $M$ , the recipient's identity  $\text{ID}_R$ , and the sender's private key  $S_{\text{ID}_S}$ , and outputs a ciphertext  $\sigma = \text{Sign/Encrypt}(M, S_{\text{ID}_S}, \text{ID}_R)$ .  
**Decrypt/Verify:** is a deterministic decryption algorithm that takes as input a ciphertext  $\sigma$ , public parameters  $\text{params}$ , the receiver's private key  $S_{\text{ID}_R}$  and (optionally) a sender's identity  $\text{ID}_S$  before returning a valid message-signature pair  $(M, s)$  or a distinguished symbol  $\perp$  if  $\sigma$  does not decrypt into a message bearing signer  $\text{ID}_S$ 's signature.

Unlike recent works of [13, 17] that present two-layer designs of probabilistic signature followed by a deterministic encryption, our construction is a single-layer construction jointly achieving signature and encryption on one side and decryption and verification on the other side. Although the description of our scheme could be modified to fit a two-layer formalism, we kept the monolithic presentation without hampering the non-repudiation property as, similarly to [13, 17], our construction enables an ordinary signature on the plaintext to be extracted from any properly formed ciphertext using the recipient's private key. The extracted message-signature pair can be forwarded to any third party in such a way that a sender remains committed to the content of the plaintext.

Unlike models of [13, 17] that consider anonymous ciphertexts, the above one assumes that senders' identities are sent in the clear along with ciphertexts. Actually, receivers do not need to have any a priori knowledge on whom the ciphertext emanates from in our scheme but this simply allows more efficient reductions in the security proofs. A simple modification of our scheme yields anonymous ciphertexts and enables senders' identities to be recovered by the Decrypt/Verify algorithm (which only takes a ciphertext and the recipient's private key as input).

**Definition 3.** *An identity-based signcryption scheme (IBSC) satisfies the **message confidentiality** property (or adaptive chosen-ciphertext security: IND-IBSC-CCA) if no PPT adversary has a non-negligible advantage in the following game.*

1. The challenger runs the **Setup** algorithm on input of a security parameter  $k$  and sends the domain-wide parameters  $\text{params}$  to the  $\mathcal{A}$ .
2. In a find stage,  $\mathcal{A}$  starts probing the following oracles:
  - **Keygen**: returns private keys associated to arbitrary identities.
  - **Sign/Encrypt**: given a pair of identities  $\text{ID}_S, \text{ID}_R$  and a plaintext  $M$ , it returns an encryption under the receiver's identity  $\text{ID}_R$  of the message  $M$  signed in the name of the sender  $\text{ID}_S$ .
  - **Decrypt/Verify**: given a pair of identities  $(\text{ID}_S, \text{ID}_R)$  and a ciphertext  $\sigma$ , it generates the receiver's private key  $S_{\text{ID}_R} = \text{Keygen}(\text{ID}_R)$  and returns either a valid message-signature pair  $(M, s)$  for the sender's identity  $\text{ID}_S$  or the  $\perp$  symbol if, under the private key  $S_{\text{ID}_R}$ ,  $\sigma$  does not decrypt into a valid message-signature pair.
3.  $\mathcal{A}$  produces two plaintexts  $M_0, M_1 \in \mathcal{M}$  and identities  $\text{ID}_S^*$  and  $\text{ID}_R^*$ . She may not have extracted the private key of  $\text{ID}_R^*$  and she obtains  $C = \text{Sign/Encrypt}(M_b, S_{\text{ID}_S^*}, \text{ID}_R^*, \text{params})$ , for a random a bit  $b \xleftarrow{R} \{0, 1\}$ .

4. In the guess stage,  $\mathcal{A}$  asks new queries as in the find stage. This time, she may not issue a key extraction request on  $ID_R^*$  and she cannot submit  $C$  to the *Decrypt/Verify* oracle for the target identity  $ID_R^*$ .
5. Finally,  $\mathcal{A}$  outputs a bit  $b'$  and wins if  $b' = b$ .

$\mathcal{A}$ 's advantage is defined as  $Adv(\mathcal{A}) := 2 \times \Pr[b' = b] - 1$ .

The next definition, given in [13], considers non-repudiation w.r.t. signatures embedded in ciphertexts rather than w.r.t. ciphertexts themselves.

**Definition 4.** An identity-based signcryption scheme (IBSC) is said to be **existentially signature-unforgeable** against adaptive chosen messages and ciphertexts attacks (ESUF-IBSC-CMA) if no PPT adversary can succeed in the following game with a non-negligible advantage:

1. the challenger runs the *Setup* algorithm on input  $k$  and gives the system-wide public key to the adversary  $\mathcal{F}$ .
2.  $\mathcal{F}$  issues a number of queries as in the previous definition.
3. Finally,  $\mathcal{F}$  outputs a triple  $(\sigma^*, ID_S^*, ID_R^*)$  and wins the game if the sender's identity  $ID_S^*$  was not corrupted and if the result of the *Decrypt/Verify* oracle on the ciphertext  $\sigma^*$  under the private key associated to  $ID_R^*$  is a valid message-signature pair  $(M^*, s^*)$  such that no *Sign/Encrypt* query involved  $M^*$ ,  $ID_S^*$  and some receiver  $ID_R'$  (possibly different from  $ID_R^*$ ) and resulted in a ciphertext  $\sigma'$  whose decryption under the private key  $S_{ID_R'}$  is the alleged forgery  $(M^*, s^*, ID_S^*)$ .

The adversary's advantage is its probability of victory.

In both of these definitions, we consider insider attacks [1]. Namely, in the definition of message confidentiality, the adversary is allowed to be challenged on a ciphertext created using a corrupted sender's private key whereas, in the notion of signature non-repudiation, the forger may output a ciphertext computed under a corrupted receiving identity.

## 4.2 The scheme

Our scheme is obtained from an optimized combination of our IBS scheme with the most basic version of the Sakai-Kasahara IBE [40, 16] which is only secure against chosen-plaintext attacks when used as an encryption-only system. This allows performing the signature-encryption operation without computing a pairing whereas only two pairings have to be computed upon decryption/verification.

**Setup:** given  $k$ , the PKG chooses bilinear map groups  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  of prime order  $p > 2^k$  and generators  $Q \in \mathbb{G}_2$ ,  $P = \psi(Q) \in \mathbb{G}_1$ ,  $g = e(P, Q) \in \mathbb{G}_T$ . It then chooses a master key  $s \xleftarrow{R} \mathbb{Z}_p^*$ , a system-wide public key  $Q_{pub} = sQ \in \mathbb{G}_2$  and hash functions  $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ ,  $H_2 : \{0, 1\}^* \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$  and  $H_3 : \mathbb{G}_T \rightarrow \{0, 1\}^n$ . The public parameters are

$$\text{params} := \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, Q, g, Q_{pub}, e, \psi, H_1, H_2, H_3\}$$



**Keygen:** for an identity  $ID$ , the private key is  $S_{ID} = \frac{1}{H_1(ID)+s}Q \in \mathbb{G}_2$ .

**Sign/Encrypt:** given a message  $M \in \{0,1\}^*$ , a receiver's identity  $ID_B$  and a sender's private key  $S_{ID_A}$ ,

1. Pick  $x \xleftarrow{R} \mathbb{Z}_p^*$ , compute  $r = g^x$  and  $c = M \oplus H_3(r) \in \{0,1\}^n$ .
2. Set  $h = H_2(M, r) \in \mathbb{Z}_p^*$ .
3. Compute  $S = (x + h)\psi(S_{ID_A})$ .
4. Compute  $T = x(H_1(ID_B)P + \psi(Q_{pub}))$ .

The ciphertext is  $\sigma = \langle c, S, T \rangle \in \{0,1\}^n \times \mathbb{G}_1 \times \mathbb{G}_1$ .

**Decrypt/Verify:** given  $\sigma = \langle c, S, T \rangle$ , and some sender's identity  $ID_A$ ,

1. Compute  $r = e(T, S_{ID_B})$ ,  $M = c \oplus H_3(r)$ , and  $h = H_2(M, r)$ .
2. Accept the message iff  $r = e(S, H_1(ID_A)Q + Q_{pub})g^{-h}$ . If this condition holds, return the message  $M$  and the signature  $(h, S) \in \mathbb{Z}_p^* \times \mathbb{G}_1$ .

If required, the anonymity property is obtained by scrambling the sender's identity  $ID_A$  together with the message at step 1 of **Sign/Encrypt** in such a way that the recipient retrieves it at the first step of the reverse operation. This change does not imply any computational penalty in practice but induces more expensive security reductions. In order for the proof to hold,  $ID_A$  must be appended to the inputs of  $H_2$ .

### 4.3 Security results

The following theorems claim the security of the scheme in the random oracle model under the same irreflexivity assumption as Boyen's scheme [13]: the signature/encryption algorithm is assumed to always take distinct identities as inputs (in other words, a principal never encrypts a message bearing his signature using his own identity).

**Theorem 2.** *Assume that an IND-IBSC-CCA adversary  $\mathcal{A}$  has an advantage  $\epsilon$  against our scheme when running in time  $\tau$ , asking  $q_{h_i}$  queries to random oracles  $H_i$  ( $i = 1, 2, 3$ ),  $q_{se}$  signature/encryption queries and  $q_{dv}$  queries to the decryption/verification oracle. Then there is an algorithm  $\mathcal{B}$  to solve the  $q$ -BDHIP for  $q = q_{h_1}$  with probability*

$$\epsilon' > \frac{\epsilon}{q_{h_1}(2q_{h_2} + q_{h_3})} \left(1 - q_{se} \frac{q_{se} + q_{h_2}}{2^k}\right) \left(1 - \frac{q_{dv}}{2^k}\right)$$

*within a time  $\tau' < \tau + O(q_{se} + q_{dv})\tau_p + O(q_{h_1}^2)\tau_{mult} + O(q_{dv}q_{h_2})\tau_{exp}$  where  $\tau_{exp}$  and  $\tau_{mult}$  are respectively the costs of an exponentiation in  $\mathbb{G}_T$  and a multiplication in  $\mathbb{G}_2$  whereas  $\tau_p$  is the complexity of a pairing computation.*

*Proof.* See appendix B. □

Again the reduction is pretty loose. However, a similar remark can be made about security proofs for IBSC schemes described in [13, 17].

**Theorem 3.** Assume there exists an ESUF-IBSC-CMA attacker  $\mathcal{A}$  that makes  $q_{h_i}$  queries to random oracles  $H_i$  ( $i = 1, 2, 3$ ),  $q_{se}$  signature/ encryption queries and  $q_{dv}$  queries to the decryption/verification oracle. Assume also that, within a time  $\tau$ ,  $\mathcal{A}$  produces a forgery with probability  $\epsilon \geq 10(q_{se} + 1)(q_{se} + q_{h_2})/2^k$ . Then, there is an algorithm  $\mathcal{B}$  that is able to solve the  $q$ -DHIP for  $q = q_{h_1}$  in expected time

$$\tau' \leq 120686q_{h_1}q_{h_2} \frac{\tau + O((q_{se} + q_{dv})\tau_p) + q_{dv}q_{h_2}\tau_{exp}}{\epsilon(1 - 1/2^k)(1 - q/2^k)} + O(q^2\tau_{mult})$$

where  $\tau_{mult}$ ,  $\tau_{exp}$  and  $\tau_p$  denote the same quantities as in theorem 2.

*Proof.* See appendix C. □

We now restate theorem 2 for the variant of our scheme with anonymous ciphertexts. The simulator's worst-case running time is affected by the fact that, when handling Decrypt/Verify requests, senders' identities are not known in advance. The reduction involves a number of pairing calculations which is quadratic in the number of adversarial queries.

**Theorem 4.** Assume that an IND-IBSC-CCA adversary  $\mathcal{A}$  has an advantage  $\epsilon$  against our scheme when running in time  $\tau$ , asking  $q_{h_i}$  queries to random oracles  $H_i$  ( $i = 1, 2, 3$ ),  $q_{se}$  signature/encryption queries and  $q_{dv}$  queries to the decryption/verification oracle. Then there is an algorithm  $\mathcal{B}$  to solve the  $q$ -BDHIP for  $q = q_{h_1}$  with probability

$$\epsilon' > \frac{\epsilon}{q_{h_1}(2q_{h_2} + q_{h_3})} \left(1 - q_{se} \frac{q_{se} + q_{h_2}}{2^k}\right) \left(1 - \frac{q_{dv}}{2^k}\right)$$

within a time  $\tau' < \tau + O(q_{se} + q_{dv}q_{h_2})\tau_p + O(q_{h_1}^2)\tau_{mult} + O(q_{dv}q_{h_2})\tau_{exp}$  where  $\tau_{exp}$ ,  $\tau_{mult}$  and  $\tau_p$  denote the same quantities as in previous theorems.

*Proof.* See appendix D. □

Theorem 3 can be similarly restated as its reduction cost is affected in the same way.

A formal proof of *ciphertext anonymity* in the model of [13] can be given under the  $q$ -BDHI assumption for the anonymous version of the scheme.

## 5 Known limitations

We concede that even the anonymous variant does not feature all the properties of the systems of Boyen [13] or Chen-Malone-Lee [17]. For example, it does not have the *ciphertext unlinkability* property [13, 17]: it seems infeasible for anyone to use his private key to embed a given message-signature pair into a proper ciphertext intended to himself. We were also unable to formally establish the *ciphertext authentication property* according to which a ciphertext is always signed

and encrypted by the same person and cannot be subject to a kind of ‘man-in-the-middle’ attack. Nevertheless, the scheme does seem to have this property because of the same reason that precludes the ciphertext unlinkability property. If we are concerned with having formal evidence that the aforementioned kind of ‘man-in-the-middle’ attack is doomed to failure, we may just turn the system into a *ciphertext unforgeable* scheme in the sense of definition 2 in [33] instead of considering non-repudiation for signatures embedded in ciphertexts as we did here. This is accomplished by simply hashing identities  $ID_A$  and  $ID_B$  along with the message  $M$  and the commitment  $r$  when computing the Fiat-Shamir-like challenge  $h$ .

Overall, we believe that the scheme does satisfy the main requirements that might be desired in practice. In our opinion, it suffices to implement most practical applications and its great efficiency renders it very attractive for identity-based cryptography. Indeed, its main disadvantage w.r.t. [13, 17], which is its reliance on the non-standard  $q$ -DHI and  $q$ -BDHI assumptions, is mostly theoretical and we do not see it as a serious problem.

## 6 Efficiency discussions and comparisons

In [42], Smart and Vercauteren pointed out problems that arise when several pairing based protocols are implemented with asymmetric pairings. They showed the difficulty of finding groups  $\mathbb{G}_2$  allowing the use of the most efficient pairing calculation techniques for ordinary curves [4] if arbitrary strings should be *efficiently* hashed onto them and efficient isomorphism  $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$  must be available at the same time. As a consequence, several protocols have to be implemented with groups for which no efficient isomorphism  $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$  is computable and their security eventually has to rely on somewhat unnatural assumptions.

Except [40] that has no security proof (and actually has several known security problems [34]), all known identity-based signcryption schemes would require to hash onto  $\mathbb{G}_2$  if they were instantiated with asymmetric pairings. Our scheme avoids this problem since it does not require to hash onto a cyclic group. It thus more easily benefits from optimized pairing calculation algorithms. For example, section 4 of [42] yields an example of group  $\mathbb{G}_2$  for which techniques of [4] can be used and where efficient isomorphisms are available.

In table 1, we assess the comparative efficiency of several identity-based signcryption schemes, implemented according to their original descriptions. Table 1 summarises the number of relevant basic operations underlying several identity-based signcryption and signature schemes, namely,  $\mathbb{G}_T$  exponentiations, scalar point multiplications, and pairing evaluations, and compares the observed processing times (in milliseconds) for a supersingular curve of embedding degree  $k = 6$  over  $\mathbb{F}_{397}$ , using implementations written in C++ and run on an Athlon XP 2 GHz. Subtleties in the algorithms determine somewhat different running times even when the operation counts for those algorithms are equal.

**Table 1.** Efficiency comparison

signcryption scheme	Sign/Encrypt				Decrypt/Verify			
	exp	mul	pairings	time (ms)	exp	mul	pairings	time (ms)
Boyen [13]	1	3	1 <sup>†</sup>	9.37		2	4 <sup>†</sup>	12.66
Chow-Yiu-Hui-Chow <sup>¶</sup> [20]		2	2 <sup>★</sup>	7.24		1	4 <sup>★</sup>	11.88
Libert-Quisquater <sup>♣♠</sup> [32]		2	2 <sup>★</sup>	7.24		1	4 <sup>★</sup>	11.88
Nalla-Reddy <sup>◇⋈</sup> [36]	1	2	1 <sup>†</sup>	8.43	1		3 <sup>†</sup>	9.06
Malone-Lee <sup>♣</sup> [33]		3	1 <sup>‡</sup>	5.47		1	3	9.06
Chen-Malone-Lee [17]		3	1 <sup>‡</sup>	5.47		1	3	9.06
Sakai-Kasahara <sup>♣</sup> [40]	2	1+1 <sup>§</sup>		6.41	1		2	9.37
Libert-Quisquater <sup>⋈</sup> [32]		3	1 <sup>‡</sup>	5.47		1	2	6.41
ours	1	2		2.65	1		2	6.09
signature scheme	Sign				Verify			
	exp	mul	pairings	time (ms)	exp	mul	pairings	time (ms)
Chow-Yiu-Hui-Chow [20]		2	1 <sup>†</sup>	3.60			2 <sup>†</sup>	6.41
Heß[30]	1	2		2.50	1		2 <sup>†</sup>	6.41
Cha-Cheon [15]		2		1.87		1	2	6.41
ours		2		1.56		1	1	3.60

(†) One pairing is precomputable, incurring for each user a storage cost of one  $\mathbb{G}_T$  element for each other user in the system.

(‡) One pairing is precomputable, incurring for each user a storage cost of one  $\mathbb{G}_T$  element for each other user in the system, plus one  $\mathbb{G}_T$  exponentiation.

(★) Two pairings are precomputable, incurring for each user a storage cost of one  $\mathbb{G}_T$  element for each user in the system, plus two  $\mathbb{G}_T$  exponentiations.

(§) One of the scalar multiplications is done in  $\langle Q \rangle$  rather than  $\langle P \rangle$  where  $(P, Q)$  generates  $E[p]$ .

(¶) Universally verifiable scheme (i.e. supports public ciphertext validation).

(♣) These schemes suffer from security problems as mentioned in [32, 34].

(♠) This scheme does not provide insider-security for the message-confidentiality criterion.

(◇) This scheme has no security proof.

(⋈) This construction can only authenticate messages from the receiver's point of view.

We see from these results that our proposed algorithms rank among the fastest schemes.

## 7 Intellectual property issues

As far as we know, neither the Sakai-Kasahara [40] key generation method or the related IBE scheme are patented. Hence, except those involved in possible implementation tricks, the techniques that we used are entirely patent-free.

## 8 Conclusion

We have described efficient and provably secure signature and signcryption schemes that are faster than any pairing-based scheme previously proposed so far in the literature. The latter signature/encryption protocol can be instantiated with either named or anonymous ciphertexts and is more convenient than previous proposals for implementations with asymmetric pairings.

## References

1. J.-H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In *Eurocrypt'02*, volume 2332 of *LNCS*, pages 83–107. Springer, 2002.
2. P. S. L. M. Barreto. The pairing based crypto lounge. <http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html>.
3. P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Asiacrypt'05*, volume 3788 of *LNCS*, pages 515–532. Springer, 2002.
4. P. S. L. M. Barreto, B. Lynn, and M. Scott. On the selection of pairing-friendly groups. In *SAC'03*, volume 3006 of *LNCS*, pages 17–25. Springer, 2003.
5. P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. Cryptology ePrint Archive, Report 2005/133, 2005. <http://eprint.iacr.org/2005/133>.
6. M. Bellare, C. Namprempe, and G. Neven. Security proofs for identity-based identification and signature schemes. In *Eurocrypt'04*, volume 3027 of *LNCS*, pages 268–286. Springer, 2004.
7. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *1st ACM Conference on Computer and Communications Security*, pages 62–73, Fairfax, USA, 1993. ACM Press.
8. D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In *Eurocrypt'04*, volume 3027 of *LNCS*, pages 223–238. Springer, 2004.
9. D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *Crypto'04*, volume 3152 of *LNCS*, pages 443–459. Springer, 2004.
10. D. Boneh and X. Boyen. Short signatures without random oracles. In *Eurocrypt'04*, volume 3027 of *LNCS*, pages 56–73. Springer, 2004.
11. D. Boneh, X. Boyen and E.-J. Goh. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In *Eurocrypt'05*, *LNCS* 3494, pp. 440–456. Springer, 2005.

12. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Crypto'01*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.
13. X. Boyen. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In *Crypto'03*, volume 2729 of *LNCS*, pages 383–399. Springer, 2003.
14. X. Boyen, B. Waters. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). To appear in *Crypto'06*, *LNCS* series, 2006.
15. J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In *PKC'03*, volume 2567 of *LNCS*, pages 18–30. Springer, 2003.
16. L. Chen and Z. Cheng. Security proof of Sakai-Kasahara's identity-based encryption scheme. Cryptology ePrint Archive, Report 2005/226, 2005. <http://eprint.iacr.org/2005/226>.
17. L. Chen and J. Malone-Lee. Improved identity-based signcryption. In *PKC'05*, volume 3386 of *LNCS*, pages 362–379. Springer, 2005.
18. J. H. Cheon. Security Analysis of the Strong Diffie-Hellman Problem. In *Eurocrypt'06*, volume 4004 of *LNCS*, pages 1–11. Springer, 2006.
19. J. H. Cheon, Y. Kim, and H. J. Yoon. A new id-based signature with batch verification. Cryptology ePrint Archive, Report 2004/131, 2004. <http://eprint.iacr.org/2004/131>.
20. S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In *6th International Conference on Information Security and Cryptology – ICISC'03*, volume 2971 of *LNCS*, pages 352–369. Springer, 2003.
21. S. S. M. Chow, T. H. Yuen, L. C. K. Hui, and S. M. Yiu. Signcryption in hierarchical identity based cryptosystem. In *20th International Conference on Information Security (SEC'05)*. IFIP TC11, 2005.
22. C. Cocks. An identity based encryption scheme based on quadratic residues. In *8th IMA International Conference*, volume 2260 of *LNCS*, pages 360–363. Springer, 2001.
23. Y. Dodis, J. Katz, S. Xu, and M. Yung. Strong key-insulated signature schemes. In *PKC'03*, volume 2567 of *LNCS*, pages 130–144. Springer, 2003.
24. Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In *PKC'05*, volume 3386 of *LNCS*, pages 416–431. Springer, 2005.
25. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Crypto'86*, volume 0263 of *LNCS*, pages 186–194. Springer, 1986.
26. C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In *Asiacrypt'02*, volume 2501 of *LNCS*, pages 548–566. Springer, 2002.
27. C. Gentry. Practical Identity-Based Encryption Without Random Oracles. In *Eurocrypt'06*, volume 4004 of *LNCS*, pages 445–464. Springer, 2006.
28. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen message attacks. *SIAM Journal of Computing*, 17(2):281–308, 1988.
29. L. Guillou and J.-J. Quisquater. A “paradoxical” identity-based signature scheme resulting from zero-knowledge. In *Crypto'88*, volume 0403 of *LNCS*, pages 216–231. Springer, 1988.
30. F. Heß. Efficient identity based signature schemes based on pairings. In *SAC'02*, volume 2595 of *LNCS*, pages 310–324. Springer, 2003.
31. K. Kurosawa and S.-H. Heng. Identity-based identification without random oracles. In *ISH'05*, *LNCS*. Springer, 2005. To appear.

32. B. Libert and J.-J. Quisquater. New identity based signcryption schemes from pairings. In *IEEE Information Theory Workshop*, Paris, France, 2003. <http://eprint.iacr.org/2003/023>.
33. J. Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002. <http://eprint.iacr.org/2002/098>.
34. N. McCullagh and P. S. L. M. Barreto. Efficient and forward-secure identity-based signcryption. Cryptology ePrint Archive, Report 2004/117, 2004. <http://eprint.iacr.org/2004/117>.
35. A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001.
36. D. Nalla and K. C. Reddy. Signcryption scheme for identity-based cryptosystems. Cryptology ePrint Archive, Report 2003/066, 2003. <http://eprint.iacr.org/2003/066>.
37. K. G. Paterson and J. C. N. Schuldt. Efficient Identity-based Signatures Secure in the Standard Model. To appear in *ACISP'06*, *LNCS* series. Springer, 2006. Also available from <http://eprint.iacr.org/2006/080>.
38. D. Pointcheval and J. Stern. Security proofs for signature schemes. In *Eurocrypt'96*, volume 1992 of *LNCS*, pages 387–398. Springer, 1996.
39. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.
40. R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. In *SCIS'03*, Hamamatsu, Japan, 2003. <http://eprint.iacr.org/2003/054>.
41. A. Shamir. Identity based cryptosystems and signature schemes. In *Crypto'84*, volume 0196 of *LNCS*, pages 47–53. Springer, 1984.
42. N. P. Smart and F. Vercauteren. On computable isomorphisms in efficient pairing based systems. Cryptology ePrint Archive, Report 2005/116, 2005. <http://eprint.iacr.org/2005/116>.
43. B. Waters. Efficient identity-based encryption without random oracles. In *Eurocrypt'05*, volume 3494 of *LNCS*, pages 114–127. Springer, 2005.
44. T. H. Yuen and V. K. Wei. Fast and proven secure blind identity-based signcryption from pairings. In *CT-RSA'05*, volume 3376 of *LNCS*, pages 305–322. Springer, 2003.
45. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *PKC'04*, volume 2947 of *LNCS*, pages 277–290. Springer, 2004.
46. Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption)  $\ll$  cost(signature) + cost(encryption). In *Crypto'97*, volume 1294 of *LNCS*, pages 165–179. Springer, 1997.

## A Proof of lemma 2

*Proof.* The proof relies on the forking lemma. We first show how to provide the adversary with a consistent view by coherently answering all of her queries and we then explain how to apply the forking lemma.

Algorithm  $\mathcal{B}$  takes as input an instance  $(P, Q, \alpha Q, \alpha^2 Q, \dots, \alpha^q Q)$  of the  $q$ -DHI problem in bilinear groups  $(\mathbb{G}_1, \mathbb{G}_2)$  and aims at finding  $\frac{1}{\alpha}P$ . In a preparation phase,  $\mathcal{B}$  builds generators  $H \in \mathbb{G}_2$ ,  $G = \psi(H) \in \mathbb{G}_1$  and a domain-wide

public key  $H_{pub} = xH \in \mathbb{G}_2$  (for some unknown element  $x \in \mathbb{Z}_p^*$ ) such that it knows  $q-1$  pairs  $(I_i, \frac{1}{I_i+x}G)$  for  $I_1, I_2, \dots, I_{q-1} \in_R \mathbb{Z}_p^*$ . To do so,

1. It randomly picks  $I^* \xleftarrow{R} \mathbb{Z}_p^*$  and  $w_1, w_2, \dots, w_{q-1} \xleftarrow{R} \mathbb{Z}_p^*$  and expands the polynomial  $f(z) = \prod_{i=1}^{q-1} (z + w_i)$  to obtain coefficients  $c_0, \dots, c_{q-1} \in \mathbb{Z}_p^*$  s.t.  $f(z) = \sum_{i=0}^{q-1} c_i z^i$ . For  $i = 1, \dots, q-1$ , it also computes  $I_i = I^* - w_i \in \mathbb{Z}_p^*$ .
2. It sets  $H = \sum_{i=0}^{q-1} c_i (\alpha^i Q) = f(\alpha)Q$  as a public generator of  $\mathbb{G}_2$  and  $G = \psi(H) = f(\alpha)P$  as a generator of  $\mathbb{G}_1$ . Another group element  $H' \in \mathbb{G}_2$  is then set to  $H' = \sum_{i=1}^q c_{i-1} (\alpha^i Q)$ . We note that  $H' = \alpha H$  although  $\mathcal{B}$  does not know  $\alpha$ .
3. For  $i = 1, \dots, q-1$ ,  $\mathcal{B}$  expands  $f_i(z) = f(z)/(z + w_i) = \sum_{i=0}^{q-2} d_i z^i$  that satisfy

$$\frac{1}{\alpha + w_i}G = \frac{f(\alpha)}{\alpha + w_i}P = f_i(\alpha)P = \sum_{i=0}^{q-2} d_i \psi(\alpha^i Q)$$

The  $q-1 = q_{h_1}-1$  pairs  $(w_i, G_i = \frac{1}{\alpha+w_i}G)$  are then computed by  $\mathcal{B}$  according to the last member of the above equation.

The system-wide public key  $H_{pub}$  is chosen as

$$H_{pub} = -H' - I^*H = (-\alpha - I^*)H$$

so that its (unknown) private key is implicitly set to  $x = -\alpha - I^* \in \mathbb{Z}_p^*$ . For all  $i \in \{1, \dots, q-1\}$ , we have  $(I_i, -G_i) = (I_i, \frac{1}{I_i+x}G)$ .

The simulator  $\mathcal{B}$  is then ready to answer  $\mathcal{F}$ 's queries throughout the simulation. It first initializes a counter  $\ell$  to 0 and launches  $\mathcal{F}$  on the input  $(H_{pub}, \text{ID}^*)$  for a randomly chosen challenge identity  $\text{ID}^* \xleftarrow{R} \{0, 1\}^*$ .

- $H_1$  queries: when  $\mathcal{F}$  probes oracle  $H_1$  on an identity  $\text{ID}$ ,  $\mathcal{B}$  returns  $I^*$  if  $\text{ID} = \text{ID}^*$ . Otherwise,  $\mathcal{B}$  increments  $\ell$  by 1 and answers  $I_\ell \in \mathbb{Z}_p^*$ . In the latter case, the pair  $(\text{ID}, -G_\ell)$  is stored in a list  $L_1$ .
- Key extraction queries for an identifier  $\text{ID} \neq \text{ID}^*$ :  $\mathcal{B}$  recovers the corresponding pair  $(\text{ID}, -G_\ell)$  in  $L_1$  for which  $-G_\ell$  was computed during the preparation phase. The latter element is returned as a private key for identifier  $\text{ID}$  and looks valid from  $\mathcal{F}$ 's view.
- Signing query: upon receiving such a query on a message-identity pair  $(M, \text{ID})$ ,  $\mathcal{B}$  picks random elements  $S \xleftarrow{R} \mathbb{G}_1$ ,  $h \xleftarrow{R} \mathbb{Z}_p^*$ , computes

$$r = e(S, Q_{\text{ID}})e(G, H)^{-h},$$

where  $Q_{\text{ID}} = H_1(\text{ID})H + H_{pub}$  is computed thanks to a value  $H_1(\text{ID})$  recovered from list  $L_1$ , and then backpatches to define the value  $H_2(M, r)$  as  $h \in \mathbb{Z}_p^*$ . This simulation is similar to those of all non-interactive honest verifier zero-knowledge proofs ( $\mathcal{B}$  of course fails if the hash value  $H_2(M, r)$  is already defined but such an event is very unlikely and its probability is taken into account in the bounds given by the forking lemma).



We have explained how to simulate  $\mathcal{F}$ 's environment in a chosen-message and given identity attack. We are ready to apply the forking lemma that essentially says the following: consider a scheme producing signatures of the form  $(M, r, h, S)$ , where each of  $r, h, S$  corresponds to one of the three moves of an honest-verifier zero-knowledge protocol. Let us assume that a chosen-message attacker  $\mathcal{F}$  forges a signature  $(M, r, h, S)$  in a time  $t$  with probability  $\epsilon \geq 10(q_s + 1)(q_s + q_h)/2^k$  ( $k$  being a security parameter so that  $h$  is uniformly taken from a set of  $2^k$  elements) when making  $q_s$  signature queries and  $q_h$  random oracle calls. If the triples  $(r, h, S)$  can be simulated without knowing the private key, then there exists a Turing machine  $\mathcal{F}'$  that uses  $\mathcal{F}$  to produce two valid signatures  $(m, r, h_1, S_1)$ ,  $(m, r, h_2, S_2)$ , with  $h_1 \neq h_2$ , in expected time  $t' \leq 120686q_h t/\epsilon$ .

In our setting, from a forger  $\mathcal{F}$ , we build an algorithm  $\mathcal{F}'$  that replays  $\mathcal{F}$  a sufficient number of times on the input  $(H_{pub}, \text{ID}^*)$  to obtain two suitably-related forgeries  $\langle M^*, r, h_1, S_1 \rangle$ ,  $\langle M^*, r, h_2, S_2 \rangle$  with  $h_1 \neq h_2$ .

The reduction then works as follows. The simulator  $\mathcal{B}$  runs  $\mathcal{F}'$  to obtain two forgeries  $\langle M^*, r, h_1, S_1 \rangle$ ,  $\langle M^*, r, h_2, S_2 \rangle$  for the same message  $M^*$  and commitment  $r$ . If both forgeries satisfy the verification equation, we obtain the relations

$$e(S_1, Q_{\text{ID}^*})e(G, H)^{-h_1} = e(S_2, Q_{\text{ID}^*})e(G, H)^{-h_2},$$

with  $Q_{\text{ID}^*} = H_1(\text{ID}^*)H + H_{pub} = (I^* + x)H = -\alpha H$ . Then, it comes that

$$e((h_1 - h_2)^{-1}(S_1 - S_2), Q_{\text{ID}^*}) = e(G, H),$$

and hence  $T^* = (h_1 - h_2)^{-1}(S_2 - S_1) = \frac{1}{\alpha}G$ . From  $T^*$ ,  $\mathcal{B}$  can proceed as in [10] to extract  $\sigma^* = \frac{1}{\alpha}P$ : it knows that  $f(z)/z = c_0/z + \sum_{i=0}^{q-2} c_i z^i$  and eventually computes

$$\sigma^* = \frac{1}{c_0} \left[ T^* - \sum_{i=0}^{q-2} c_i \psi(\alpha^i Q) \right] = \frac{1}{\alpha}P$$

which is returned as a result.

It finally comes that, if  $\mathcal{F}$  forges a signature in a time  $t$  with probability  $\epsilon \geq 10(q_s + 1)(q_s + q_{h_2})/2^k$ ,  $\mathcal{B}$  solves the  $p$ -DHIP in expected time

$$t' \leq 120686q_{h_2}(t + O(q_s \tau_p))/\epsilon + O(q_{h_1}^2 \tau_{mult})$$

where the last term accounts for the cost of the preparation phase.  $\square$

## B Proof of Theorem 2

*Proof.* Algorithm  $\mathcal{B}$  takes as input  $\langle P, Q, \alpha Q, \alpha^2 Q, \dots, \alpha^q Q \rangle$  and attempts to extract  $e(P, Q)^{1/\alpha}$  from its interaction with  $\mathcal{A}$ .

In a preparation phase,  $\mathcal{B}$  selects  $\ell \xleftarrow{R} \{1, \dots, q_{h_1}\}$ , elements  $I_\ell \xleftarrow{R} \mathbb{Z}_p^*$  and  $w_1, \dots, w_{\ell-1}, w_{\ell+1}, \dots, w_q \xleftarrow{R} \mathbb{Z}_p^*$ . For  $i = 1, \dots, \ell - 1, \ell + 1, \dots, q$ , it computes  $I_i = I_\ell - w_i$ . As in the technique of [10] and in lemma 2, it sets up generators  $G_2 \in \mathbb{G}_2$ ,  $G_1 = \psi(G_2) \in \mathbb{G}_1$  and another  $\mathbb{G}_2$  element  $U = \alpha G_2$  such that it knows

$q - 1$  pairs  $(w_i, H_i = (1/(w_i + \alpha))G_2)$  for  $i \in \{1, \dots, q\} \setminus \{\ell\}$ . The system-wide public key  $Q_{pub}$  is chosen as

$$Q_{pub} = -U - I_\ell G_2 = (-\alpha - I_\ell)G_2$$

so that its (unknown) private key is implicitly set to  $x = -\alpha - I_\ell \in \mathbb{Z}_p^*$ . For all  $i \in \{1, \dots, q\} \setminus \{\ell\}$ , we have  $(I_i, -H_i) = (I_i, (1/(I_i + x))G_2)$ .

$\mathcal{B}$  then initializes a counter  $\nu$  to 1 and starts  $\mathcal{A}$  on input of  $(G_1, G_2, Q_{pub})$ . Throughout the game, we assume that  $H_1$ -queries are distinct, that the target identity  $ID_R^*$  is submitted to  $H_1$  at some point and that any query involving an identity  $ID$  comes after a  $H_1$ -query on  $ID$ :

- $H_1$ -queries (let us call  $ID_\nu$  the input of the  $\nu^{th}$  one of such queries):  $\mathcal{B}$  answers  $I_\nu$  and increments  $\nu$ .
- $H_2$ -queries on input  $(M, r)$ :  $\mathcal{B}$  returns the defined value if it exists and a random  $h_2 \xleftarrow{R} \mathbb{Z}_p^*$  otherwise. To anticipate possible subsequent Decrypt/Verify requests,  $\mathcal{B}$  additionally simulates random oracle  $H_3$  on its own to obtain  $h_3 = H_3(r) \in \{0, 1\}^n$  and stores the information  $(M, r, h_2, c = M \oplus h_3, \gamma = r \cdot e(G_1, G_2)^{h_2})$  in  $L_2$ .
- $H_3$ -queries for an input  $r \in \mathbb{G}_T$ :  $\mathcal{B}$  returns the previously assigned value if it exists and a random  $h_3 \xleftarrow{R} \{0, 1\}^n$  otherwise. In the latter case, the input  $r$  and the response  $h_3$  are stored in a list  $L_3$ .
- Keygen queries on an input  $ID_\nu$ : if  $\nu = \ell$ , then  $\mathcal{B}$  fails. Otherwise, it knows that  $H_1(ID_\nu) = I_\nu$  and returns  $-H_\nu = (1/(I_\nu + x))G_2 \in \mathbb{G}_2$ .
- Sign/Encrypt queries for a plaintext  $M$  and identities  $(ID_S, ID_R) = (ID_\mu, ID_\nu)$  for  $\mu, \nu \in \{1, \dots, q_{h_1}\}$ : we observe that, if  $\mu \neq \ell$ ,  $\mathcal{B}$  knows the sender's private key  $S_{ID_\mu} = -H_\mu$  and can answer the query according to the specification of Sign/Encrypt. We thus assume  $\mu = \ell$  and hence  $\nu \neq \ell$  by the irreflexivity assumption. Observe that  $\mathcal{B}$  knows the receiver's private key  $S_{ID_\nu} = -H_\nu$  by construction. The difficulty is to find a random triple  $(S, T, h) \in \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{Z}_p^*$  for which

$$e(T, S_{ID_\nu}) = e(S, Q_{ID_\ell})e(G_1, G_2)^{-h} \quad (1)$$

where  $Q_{ID_\ell} = I_\ell G_2 + Q_{pub}$ . To do so,  $\mathcal{B}$  randomly chooses  $t, h \xleftarrow{R} \mathbb{Z}_p^*$  and computes  $S = t\psi(S_{ID_\nu}) = -t\psi(H_\nu)$ ,  $T = t\psi(Q_{ID_\ell}) - h\psi(Q_{ID_\nu})$  where  $Q_{ID_\nu} = I_\nu G_2 + Q_{pub}$  in order to obtain the desired equality  $r = e(T, S_{ID_\nu}) = e(S, Q_{ID_\ell})e(G_1, G_2)^{-h} = e(\psi(S_{ID_\nu}), Q_{ID_\ell})^t e(G_1, G_2)^{-h}$  before patching the hash value  $H_2(M, r)$  to  $h$  ( $\mathcal{B}$  fails if  $H_2$  is already defined but this only happens with probability  $(q_{se} + q_{h_2})/2^k$ ). The ciphertext  $\sigma = \langle M \oplus H_3(r), S, T \rangle$  is returned.

- Decrypt/Verify queries on a ciphertext  $\sigma = \langle c, S, T \rangle$  for identities  $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ : we assume that  $\nu = \ell$  (and hence  $\mu \neq \ell$  by the irreflexivity assumption), because otherwise  $\mathcal{B}$  knows the receiver's private key  $S_{ID_\nu} = -H_\nu$  and can normally run the Decrypt/Verify algorithm. Since  $\mu \neq \ell$ ,  $\mathcal{B}$  has the sender's private key  $S_{ID_\mu}$  and also knows that, for all valid ciphertexts,  $\log_{S_{ID_\mu}}(\psi^{-1}(S) - hS_{ID_\mu}) = \log_{\psi(Q_{ID_\nu})}(T)$ , where  $h = H_2(M, r)$  is the

hash value obtained in the Sign/Encrypt algorithm and  $Q_{ID_\nu} = I_\nu G_2 + Q_{pub}$ . Hence, we have the relation

$$e(T, S_{ID_\mu}) = e(\psi(Q_{ID_\nu}), \psi^{-1}(S) - hS_{ID_\mu}) \quad (2)$$

which yields  $e(T, S_{ID_\mu}) = e(\psi(Q_{ID_\nu}), \psi^{-1}(S))e(\psi(Q_{ID_\nu}), S_{ID_\mu})^{-h}$ . We observe that the latter equality can be tested without inverting  $\psi$  as  $e(\psi(Q_{ID_\nu}), \psi^{-1}(S)) = e(S, Q_{ID_\nu})$ . The query is thus handled by computing  $\gamma = e(S, Q_{ID_\mu})$ , where  $Q_{ID_\mu} = I_\mu G_2 + Q_{pub}$ , and searching through list  $L_2$  for entries of the form  $(M_i, r_i, h_{2,i}, c, \gamma)$  indexed by  $i \in \{1, \dots, q_{h_2}\}$ . If none is found,  $\sigma$  is rejected. Otherwise, each one of them is further examined: for the corresponding indexes,  $\mathcal{B}$  checks if

$$e(T, S_{ID_\mu})/e(S, Q_{ID_\nu}) = e(\psi(Q_{ID_\nu}), S_{ID_\mu})^{-h_{2,i}} \quad (3)$$

(the pairings are computed only once and at most  $q_{h_2}$  exponentiations are needed), meaning that (2) is satisfied. If the unique  $i \in \{1, \dots, q_{h_2}\}$  satisfying (3) is detected, the matching pair  $(M_i, \langle h_{2,i}, S \rangle)$  is returned. Otherwise,  $\sigma$  is rejected. Overall, an inappropriate rejection occurs with probability smaller than  $q_{dv}/2^k$  across the whole game.

At the challenge phase,  $\mathcal{A}$  outputs messages  $(M_0, M_1)$  and identities  $(ID_S, ID_R)$  for which she never obtained  $ID_R$ 's private key. If  $ID_R \neq ID_\ell$ ,  $\mathcal{B}$  aborts. Otherwise, it picks  $\xi \xleftarrow{R} \mathbb{Z}_p^*$ ,  $c \xleftarrow{R} \{0, 1\}^n$  and  $S \xleftarrow{R} \mathbb{G}_1$  to return the challenge  $\sigma^* = \langle c, S, T \rangle$  where  $T = -\xi G_1 \in \mathbb{G}_1$ . If we define  $\rho = \xi/\alpha$  and since  $x = -\alpha - I_\ell$ , we can check that

$$T = -\xi G_1 = -\alpha \rho G_1 = (I_\ell + x)\rho G_1 = \rho I_\ell G_1 + \rho \psi(Q_{pub}).$$

$\mathcal{A}$  cannot recognize that  $\sigma^*$  is not a proper ciphertext unless she queries  $H_2$  or  $H_3$  on  $e(G_1, G_2)^\rho$ . Along the guess stage, her view is simulated as before and her eventual output is ignored. Standard arguments can show that a successful  $\mathcal{A}$  is very likely to query  $H_2$  or  $H_3$  on the input  $e(G_1, G_2)^\rho$  if the simulation is indistinguishable from a real attack environment.

To produce a result,  $\mathcal{B}$  fetches a random entry  $(M, r, h_2, c, \gamma)$  or  $\langle r, \cdot \rangle$  from the lists  $L_2$  or  $L_3$ . With probability  $1/(2q_{h_2} + q_{h_3})$  (as  $L_3$  contains no more than  $q_{h_2} + q_{h_3}$  records by construction), the chosen entry will contain the right element  $r = e(G_1, G_2)^\rho = e(P, Q)^{f(\alpha)^2 \xi / \alpha}$ , where  $f(z) = \sum_{i=0}^{q-1} c_i z^i$  is the polynomial for which  $G_2 = f(\alpha)Q$ . The  $q$ -BDHIP solution can be extracted by noting that, if  $\gamma^* = e(P, Q)^{1/\alpha}$ , then

$$e(G_1, G_2)^{1/\alpha} = \gamma^{*(c_0^2)} e\left(\sum_{i=0}^{q-2} c_{i+1}(\alpha^i P), c_0 Q\right) e\left(G_1, \sum_{j=0}^{q-2} c_{j+1}(\alpha^j) Q\right).$$

In an analysis of  $\mathcal{B}$ 's advantage, we note that it only fails in providing a consistent simulation because one of the following independent events:

- $E_1$ :  $\mathcal{A}$  does not choose to be challenged on  $ID_\ell$ .
- $E_2$ : a key extraction query is made on  $ID_\ell$ .

$E_3$ :  $\mathcal{B}$  aborts in a **Sign/Encrypt** query because of a collision on  $H_2$ .

$E_4$ :  $\mathcal{B}$  rejects a valid ciphertext at some point of the game.

We clearly have  $\Pr[\neg E_1] = 1/q_{h_1}$  and we know that  $\neg E_1$  implies  $\neg E_2$ . We also already observed that  $\Pr[E_3] \leq q_{se}(q_{se} + q_{h_2})/2^k$  and  $\Pr[E_4] \leq q_{dv}/2^k$ . We thus find that

$$\Pr[\neg E_1 \wedge \neg E_3 \wedge \neg E_4] \geq \frac{1}{q_{h_1}} \left(1 - q_{se} \frac{q_{se} + q_{h_2}}{2^k}\right) \left(1 - \frac{q_{dv}}{2^k}\right).$$

We obtain the announced bound by noting that  $\mathcal{B}$  selects the correct element from  $L_2$  or  $L_3$  with probability  $1/(2q_{h_2} + q_{h_3})$ . Its workload is dominated by  $O(q_{h_1}^2)$  multiplications in the preparation phase,  $O(q_{se} + q_{dv})$  pairing calculations and  $O(q_{dv}q_{h_2})$  exponentiations in  $\mathbb{G}_T$  in its emulation of the **Sign/Encrypt** and **Decrypt/Verify** oracles.  $\square$

### C Proof of Theorem 3

*Proof.* The proof is almost similar to the one of theorem 1. Namely, it shows that a forger in the ESUF-IBSC-CMA game implies a forger in a chosen-message and *given* identity attack. Using the forking lemma [38, 39], the latter is in turn shown to imply an algorithm to solve the  $q$ -Diffie-Hellman Inversion problem. More precisely, queries to the **Sign/Encrypt** and **Decrypt/Verify** oracles are answered as in the proof of theorem 2 and, at the outset of the game, the simulator chooses public parameters in such a way that it can extract private keys associated to any identity but the one which is given as a challenge to the adversary. By doing so, thanks to the irreflexivity assumption, it is able to extract clear message-signature pairs from ciphertexts produced by the forger (as it knows the private key of the receiving identity  $ID_R^*$ ).  $\square$

### D Proof of Theorem 4

*Proof.* The simulator is the same as in theorem 2 with the following differences (recall that senders' identities are provided as inputs to  $H_2$ ).

- $H_2$ -queries on input  $(ID_S, M, r)$ :  $\mathcal{B}$  returns the previously defined value if it exists and a random  $h_2 \xleftarrow{R} \mathbb{Z}_p^*$  otherwise. To anticipate subsequent **Decrypt/Verify** requests,  $\mathcal{B}$  simulates oracle  $H_3$  to obtain  $h_3 = H_3(r) \in \{0, 1\}^{n+n_0}$  (where  $n_0$  is the maximum length of identity strings) and stores  $(ID_S, M, r, h_2, c = (M \| ID_S) \oplus h_3, \gamma = r \cdot e(G_1, G_2)^{h_2})$  in list  $L_2$ .
- **Decrypt/Verify** queries: given a ciphertext  $\sigma = \langle c, S, T \rangle$  and a receiver's identity  $ID_R = ID_\nu$ , we assume that  $\nu = \ell$  because otherwise  $\mathcal{B}$  knows the receiver's private key. The simulator  $\mathcal{B}$  does not know the sender's identity  $ID_S$  but knows that  $ID_S \neq ID_\nu$ . It also knows that, for the private key  $S_{ID_S}$ ,  $\log_{S_{ID_S}}(\psi^{-1}(S) - hS_{ID_S}) = \log_{\psi(Q_{ID_\nu})}(T)$ , and hence

$$e(T, S_{ID_S}) = e(\psi(Q_{ID_\nu}), \psi^{-1}(S) - hS_{ID_S}), \quad (4)$$

where  $h = H_2(\text{ID}_S, M, r)$  is the hash value obtained in the **Sign/ Encrypt** algorithm and  $Q_{\text{ID}_\nu} = I_\nu G_2 + Q_{\text{pub}}$ . The query is handled by searching through list  $L_2$  for entries of the form  $(\text{ID}_{S,i}, M_i, r_i, h_{2,i}, c, \gamma_i)$  indexed by  $i \in \{1, \dots, q_{h_2}\}$ . If none is found, the ciphertext is rejected. Otherwise, each one of these entries for which  $\text{ID}_{S,i} \neq \text{ID}_\nu$  is further examined by checking whether  $\gamma_i = e(S, H_1(\text{ID}_{S,i})Q + Q_{\text{pub}})$  and

$$e(T, S_{\text{ID}_{S,i}})/e(S, Q_{\text{ID}_\nu}) = e(\psi(Q_{\text{ID}_\nu}), S_{\text{ID}_{S,i}})^{-h_{2,i}}. \quad (5)$$

(at most  $3q_{h_2} + 1$  pairings and  $q_{h_2}$  exponentiations must be computed), meaning that equation (4) is satisfied and that the ciphertext contains a valid message signature pair if both relations hold. If  $\mathcal{B}$  detects an index  $i \in \{1, \dots, q_{h_2}\}$  satisfying them, the matching pair  $(M_i, \langle h_{2,i}, S \rangle)$  is returned. Otherwise,  $\sigma$  is rejected and such a wrong rejection again occurs with an overall probability smaller than  $q_{dv}/2^k$ .  $\square$

## E The Kurosawa-Heng identity-based signature

We describe here the IBS scheme that can be derived from a modification of the Kurosawa-Heng [31] identity-based identification scheme using the Fiat-Shamir heuristic [25].

**Setup** and **Keygen** are the same as in our scheme described in section 3. The public parameters are

$$\text{params} := \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, Q, g, Q_{\text{pub}}, e, \psi, H_1, H_2\}.$$

We also define  $Q_{\text{ID}} = H_1(\text{ID})Q + Q_{\text{pub}}$ .

**Sign:** to sign a message  $M \in \{0, 1\}^*$ , the signer does the following:

1. picks  $x \xleftarrow{R} \mathbb{Z}_p^*$  and computes  $r = e(P, Q_{\text{ID}})^x \in \mathbb{G}_T$ ,
2. sets  $h = H_2(M, r) \in \mathbb{Z}_p^*$ ,
3. computes  $S = xP + hS_{\text{ID}}$ .

The signature on  $M$  is  $\sigma = (h, S) \in \mathbb{Z}_p^* \times \mathbb{G}_1$ .

**Verify:** a signature  $\sigma = (h, S)$  on a message  $M$  is accepted iff

$$h = H_2(M, e(S, Q_{\text{ID}})g^{-h}).$$

The above IBS can be proven secure under the  $q$ -Strong Diffie-Hellman assumption. Even in its optimized version where  $e(P, H_1(\text{ID})Q + Q_{\text{pub}})$  is pre-computed by the signer, its signature generation algorithm happens to be slightly more expensive than our scheme's one which requires a simple scalar multiplication at step 3.